МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по практическим работам
для обучающихся по направлению
10.03.01 «Информационная безопасность»

Севастополь
СевГУ
2025

УДК 004.056.5:004.413.4(076.5)
ББК 32.973-018.2я73
У677

Р е ц е н з е н т :
Ю. Ю. Эндрижикевич - д-р. техн. наук, доцент,
профессор кафедры «Информационная безопасность»

Составитель: Е. А. Контылева

У677 Управление рисками информационной безопасности : учебно-методическое пособие по практическим работам для обучающихся по направлению 10.03.01 «Информационная безопасность» / Севастопольский государственный университет ; сост.: Е. А. Контылева. – Севастополь : СевГУ, 2025. – 29 с. – Текст : электронный.

Рассмотрены теоретические материалы и требования к выполнению практических работ. Данное пособие может быть использовано для самостоятельной подготовки студентов очной и очно-заочной форм обучения направления подготовки 10.03.01 «Информационная безопасность».

УДК 004.056.5:004.413.4(076.5)
ББК 32.973-018.2я73

Рассмотрено и рекомендовано к изданию на заседании кафедры «Информационная безопасность», протокол № 9 от 27 марта 2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В данном учебно-методическом пособии определяются: область применения и границ процесса менеджмента риска информационной безопасности, установление ценности активов и оценка влияния, сценарии инцидентов, оценка и обработка рисков информационной безопасности.

Цель данного учебно-методического пособия – дать необходимый теоретический материал и требования по выполнению практических работ по дисциплине «Угрозы и риски в информационной безопасности».

Практическая работа № 1
ОПРЕДЕЛЕНИЕ ОБЛАСТИ ПРИМЕНЕНИЯ И ГРАНИЦ ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы – получить навык определения области применения и границ процесса менеджмента риска информационной безопасности.

Теоретические сведения

1 Анализ организации

Анализ организации. Изучение организации дает возможность воспроизвести характерные элементы, определяющие особенности организации. Оно касается цели, бизнеса, назначения, ценностей и стратегий этой организации, которые должны быть определены наряду с элементами, способствующими их разработке (например, заключение контрагентских договоров).

Трудность такой деятельности заключается в полном понимании структуры организации.

Определение ее реальной структуры дает понимание роли и значимости каждого подразделения в достижении целей организации.

Пример - Тот факт, что ответственный за ИБ отчитывается перед высшим руководством, а не перед руководством ИТ, может указывать на участие высшего руководства в проблемах ИБ.

Основная цель организации. Основная цель организации может определяться сферой ее деятельности, сегментом рынка и др.

Бизнес организации. Бизнес организации, определяемый техническими приемами, применяемыми ее сотрудниками и накопленным ими опытом (ноухау), дает ей возможность реализовывать свое назначение. Он является специфичной областью деятельности организации и зачастую определяет культуру ее труда.

Назначение организации. Организация достигает своей цели посредством реализации своего назначения. Для определения ее назначения должны быть определены предоставляемые сервисы и/или производимая продукция.

Ценность организации. Ценностями являются основные нормы или четко определенный кодекс поведения, выполняемые для осуществления бизнеса. Это может касаться персонала, отношений с внешними сторонами (например, клиентами), качества поставляемой продукции или предоставляемых сервисов.

Пример - Рассмотрим организацию, целью которой является предоставление услуг населению, бизнесом - транспортные услуги, а назначение заключается в перевозке детей в школу и обратно.

Ее ценностями могут быть пунктуальность предоставления услуг и безопасность перевозок.

Структура организации. Существуют разные типы структур:

– филиальная структура, в которой каждое подразделение работает под началом руководителя подразделения, ответственного за принятие стратегических, административных и операционных решений, касающихся его подразделения;

– функциональная структура, в которой функциональные полномочия осуществляются относительно процедур, характера работы и, иногда, принятия решений или составления планов (например производство, ИТ, кадры, маркетинг и т.д.).

Замечания:

– подразделение, существующее в пределах организации с филиальной структурой, может быть организовано как функциональная структура и наоборот;

– структура организации, имеющей элементы обоих типов структуры, называется матричной.

При любой организационной структуре могут различаться следующие уровни:

– уровень принятия решений (определение стратегической ориентации);

– уровень руководства (координация и менеджмент);

– операционный уровень (виды деятельности, связанные с производством и поддержкой).

Диаграмма организации. Структура организации представляется схематически в виде диаграммы организации. При таком представлении следует выделять линии отчетности и делегирования полномочий, кроме того, следует также включать в диаграмму и другие связи, которые, даже если они не основываются на каких-либо формальных полномочиях, являются тем не менее линиями информационного потока.

Стратегия организации. Для нее требуется формальное выражение руководящих принципов организации. Стратегия определяет направление и развитие организации, необходимые для извлечения выгоды из задач, стоящих перед ее бизнесом и планируемых ею основных изменений.

2 Перечень ограничений, влияющих на организацию

Следует учитывать все ограничения, влияющие на организацию и определяющие направленность ее ИБ. Источник ограничений может находиться в пределах организации, и в этом случае она имеет некоторый контроль над ними, или за пределами организации и, следовательно, не может контролироваться. Наиболее важными являются ограничения ресурсов (бюджетных, кадровых) и ограничения, связанные с чрезвычайными обстоятельствами.

Организация устанавливает свои цели (касающиеся ее бизнеса, режима работы и т.д.), способствующие выбору ее пути, возможно, на длительный период времени. Она определяет, какой организацией она хочет стать, и выбирает средства, которые для этого потребуются. При выборе своего пути организация учитывает эволюцию методов и ноу-хау, пожелания пользователей, клиентов и др. Этот путь может быть выражен в форме стратегий эксплуатации или разработки с намерением, например снизить эксплуатационные расходы, повысить качество обслуживания и т.д.

Такие стратегии, вероятно, будут включать в себя информацию и информационные системы, способствующие их реализации. Следовательно, свойства, касающиеся особенностей, назначения и стратегий организации, являются основополагающими элементами в анализе проблемы, поскольку нарушение аспекта ИБ может привести к переосмыслению целей этих стратегий. Кроме того, важно, чтобы предложения, касающиеся требований ИБ, находились в соответствии с правилами, режимами эксплуатации и средствами, применяемыми в организации.

Перечень включает в себя, но не ограничивается, следующие ограничения.

Ограничения политического свойства. Они могут касаться правительственной администрации, общественных учреждений или любой организации, которая должна применять решения, принятые на государственном уровне. Такими обычно являются решения, касающиеся стратегии или эксплуатационной направленности, принятые правительственным подразделением или организацией, уполномоченной в соответствии с законодательством принимать решения, и которые должны быть выполнены.

Пример - Компьютеризация счетов или административных документов влечет за собой проблемы с информационной безопасностью.

Ограничения стратегического свойства. Они могут возникать в результате запланированных или возможных изменений структуры или направленности организации. Они могут отражаться в стратегических или эксплуатационных планах организации.

Пример - Международное сотрудничество в области совместного использования чувствительной информации может потребовать соглашений, касающихся безопасного обмена.

Территориальные ограничения. Структура и/или цель организации могут обусловливать определенные ограничения, такие, как распределение рабочих площадок по территории своей страны или за рубежом.

Пример - Включают в себя почтовую службу, посольства, банки, филиалы крупной промышленной группы и т.д.

Ограничения, на возникновение которых влияет состояние экономики и политики.

Функционирование организации может сильно изменяться вследствие определенных событий, таких, как забастовки или национальные или международные кризисы.

Пример - Некоторые сервисы могут продолжать функционирование даже во время серьезных кризисных ситуаций.

Структурные ограничения. Тип структуры организации (филиальная, функциональная или другая) может иметь следствием определенную политику ИБ и организацию безопасности, адаптированную к структуре.

Пример - Международная структура должна быть способна приводить в соответствие требования безопасности, принятые в каждой отдельной стране.

Функциональные ограничения. Функциональные ограничения возникают непосредственно из основного или специфического назначения организации.

Пример - Организация, работающая круглосуточно, должна непрерывно обеспечивать доступность своих ресурсов.

Ограничения, касающиеся персонала. Природа этих ограничений значительным образом варьируется. Они связаны с уровнем ответственности, наймом сотрудников, квалификацией, обучением, осведомленностью в вопросах безопасности, мотивацией, доступностью и т.д.

Пример - Персонал оборонной организации должен иметь соответствующий допуск к обработке информации ограниченного доступа.

Ограничения, проистекающие из списка дел организации. Такие ограничения могут быть результатом реструктуризации или планирования новых национальных или международных политик, с установлением определенных конечных сроков.

Пример - Создание службы безопасности.

Ограничения, связанные с методами. Методы, соответствующие ноу-хау организации, необходимо устанавливать в отношении таких аспектов, как планирование проекта, технические условия, разработка и т.д.

Пример - Типичным ограничением такого рода является необходимость включения правовых обязательств организации в политику безопасности.

Ограничения культурного свойства. В некоторых организациях рабочие традиции или основной бизнес привели к созданию определенной культуры организации, которая может быть несовместима с мерами и средствами контроля и управления безопасностью. Такая культура является основной эталонной системой персонала и может определяться многими аспектами, включающими в себя образование, обучение, профессиональный опыт, работу, на которую распространяется жизненный опыт, мнения, философию, убеждения, чувства, социальный статус и т.д.

Бюджетные ограничения. Рекомендуемые меры и средства контроля и управления безопасностью могут иметь иногда очень высокую стоимость. Несмотря на то, что не всегда уместно строить инвестирование безопасности на экономической эффективности, финансовые отделы организации требуют, как правило, экономического обоснования.

Пример - В организациях частного сектора и некоторых общественных организациях совокупные расходы на меры и средства контроля и управления безопасностью не должны превышать издержек от возможных последствий рисков. Высшее руководство должно поэтому оценивать и принимать просчитанные риски, если оно желает избежать чрезмерных расходов, связанных с обеспечением безопасности.

3 Перечень законодательных и нормативных положений, имеющих отношение к деятельности организации

Должны определяться нормативные требования, имеющие отношение к видам деятельности организации. К их числу могут быть отнесены законы, постановления, специальные инструкции, относящиеся к сфере деятельности организации или внутренним/внешним нормам. Это касается также договоров и соглашений и, в общем, любых обязательств юридического свойства.

4 Перечень ограничений, влияющих на область применения

При определении ограничений желательно перечислить те из них, которые влияют на область применения, и определить те, на которые возможно некоторое воздействие. Они добавляются к ограничениям организации, перечисленным выше, и, возможно, могут изменить их. Далее представляется

перечень возможных типов ограничений, который не является исчерпывающим.

Ограничения, возникающие из ранее существовавших процессов. Проекты приложений не обязательно разрабатываются одновременно. Некоторые из них зависят от ранее существовавших процессов. Даже если процесс может быть разбит на подпроцессы, не обязательно на данный процесс будут влиять все подпроцессы другого процесса.

Технические ограничения. Технические ограничения, относящиеся к инфраструктуре, в основном возникают от установленных аппаратных и программных средств, а также от помещений или площадок, где осуществляются процессы:

– архивы (файлы) - требования, касающиеся организации, менеджмент носителей, менеджмент правил доступа и т.д.;

– общая архитектура - требования, касающиеся топологии (централизованная, распределенная, клиент- сервер), физическая архитектура и т.д.;

– прикладные программы - требования, касающиеся проектирования специфичного программного обеспечения, рыночные стандарты и т.д.;

– пакеты программ - требования, касающиеся стандартов, уровня оценки, качества, соответствия нормам, безопасности и т.д.;

– аппаратные средства - требования, касающиеся стандартов, качества, соответствия нормам и т.д.;

– сети связи - требования, касающиеся покрытия, стандартов, емкости, надежности и т.д.;

– инфраструктура сооружений и инженерных коммуникаций - требования, касающиеся гражданского строительства, конструкций, высокого напряжения, низкого напряжения и т.д.

Финансовые ограничения. Реализация мер и средств контроля и управления безопасностью часто ограничивается тем бюджетом, который может выделить организация. Однако финансовое ограничение должно по-прежнему оставаться последним, подлежащим рассмотрению, поскольку вопрос о выделении бюджетных средств на безопасность может быть решен на основе анализа безопасности.

Ограничения, связанные со средой. Они обусловлены географической или экономической средой, в которых процессы реализуются: страна, климат, природные риски, территориальное расположение, состояние экономики и др. Ограничения по времени. Время, необходимое для реализации мер и средств контроля и управления безопасностью, должно определяться с учетом возможности модернизации информационной системы. Если на реализацию

затрачивается очень много времени, то риски, для которых разрабатывались меры и средства контроля и управления, могут измениться. Время является определяющим фактором при принятии решений и выборе приоритетов.

Ограничения, касающиеся методов. Методы, соответствующие ноу-хау организации, должны использоваться в отношении планирования проекта, технических условий, разработки и др.

Организационные ограничения. Различные ограничения могут следовать из требований организации, а именно:

– эксплуатация - требования, касающиеся длительности производственного цикла, предоставления услуг, наблюдения, мониторинга, планов действий в чрезвычайных ситуациях, ухудшения работы и др.;

– поддержка - требования к поиску неисправностей, связанных с инцидентом, превентивным действиям, быстрому исправлению и др.;

– менеджмент кадровых ресурсов - требования, касающиеся обучения операторов и пользователей, квалификации, необходимой для таких должностей, как системный администратор или администратор данных и др.;

– административный менеджмент - требования, касающиеся обязанностей и др.;

– менеджмент разработки - требования, касающиеся инструментальных средств разработки, систем автоматизированной разработки программ, планов приемочного контроля, обеспечения

организации и др.;

– менеджмент внешних отношений - требования, касающиеся формирования отношений с третьими сторонами, договоров и т.д.

Ход работы

Для своей организации или организации из числа предложенных, на основании приведенных выше теоретических сведений выполнить следующие задачи:

1. Провести анализ организации
2. Сформировать перечень ограничений, влияющих на организацию
3. Сформировать перечень законодательных и нормативных положений, имеющих отношение к деятельности организации
4. Сформировать перечень ограничений, влияющих на область применения.

Результат выполнения оформить в виде отчёта под названием *ИвановИИ.pdf*.

Практическая работа № 2
ОПРЕДЕЛЕНИЕ И УСТАНОВЛЕНИЕ ЦЕННОСТИ АКТИВОВ И ОЦЕНКА ВЛИЯНИЯ

Цель работы – получить навык определения и установления ценности активов и оценки влияния.

Теоретические сведения

1. Примеры определения активов

Для установления ценности активов организация должна в первую очередь определить все свои активы на соответствующем уровне детализации. Могут различаться два вида активов:

– основные активы, включающие бизнес-процессы, бизнес-деятельность и информацию;

– вспомогательные (поддерживающие) активы, от которых зависят основные составные части области применения всех типов, включающие аппаратные средства, программное обеспечение, сеть, персонал, место функционирования организации, структуру организации.

1.1 Определение основных активов

Данная деятельность заключается в определении основных активов (бизнес-процессы и бизнесдеятельность, информация). Такое определение осуществляется сотрудниками совместной рабочей группы, участвующими в процессе (руководители, специалисты в сфере информационных систем и пользователи).

Основными активами обычно являются базовые процессы и информация о деятельности организации в ее сфере действия. Могут рассматриваться также и другие основные активы, такие, как процессы жизнедеятельности организации, которые будут иметь отношение к формированию политики ИБ или плана непрерывности бизнеса. В зависимости от цели, иногда не требуется исчерпывающий анализ всех элементов, входящих в процесс менеджмента риска. В таких случаях рамки изучения могут быть ограничены наиболее значимыми элементами.

Основные активы бывают двух типов.

1. Бизнес-процессы (или подпроцессы) и бизнес-деятельность, например:

– процессы, утрата или ухудшение которых делает невозможным реализацию целей и задач организации;

– процессы, содержащие засекреченные процессы или процессы, созданные с использованием патентованной технологии;

– процессы, модификация которых может значительно повлиять на реализацию целей и задач организации;

– процессы, которые необходимы организации для выполнения договорных, законодательных или нормативных требований.

2. Информация. Основная информация включает в себя:

– информацию, необходимую для реализации назначения или бизнеса организации;

– информацию личного характера, которая определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни;

– стратегическую информацию, необходимую для достижения целей, определяемых направлением стратегии организации;

– ценную информацию, сбор, хранение, обработка и передача которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение.

Процессы и информация, которые не были определены как чувствительные относительно данной деятельности, не будут иметь определенной классификации в оставшейся части исследования. Это означает, что если такие процессы или информация будут скомпрометированы, организация по-прежнему будет успешно осуществлять свое назначение. Тем не менее они часто наследуют меры и средства контроля и управления, реализуемые для защиты процессов и информации, определенных как чувствительные.

1.2 Перечень и описание вспомогательных активов

Сфера рассмотрения включает активы, которые должны быть определены и описаны. Этим активам присущи уязвимости, которые могут быть использованы угрозами, нацеленными на порчу основных активов сферы рассмотрения (процессов и информации). Они могут быть различных типов.

Аппаратные средства. Тип "аппаратные средства" включает все физические элементы, поддерживающие процессы. Аппаратура обработки данных (активная). Аппаратура автоматизированной обработки информации состоит из элементов, необходимых для независимой работы.

Мобильная аппаратура. Портативная вычислительная техника.

Пример - Портативный компьютер (ноутбук), карманный компьютер.

Стационарная аппаратура. Вычислительная техника, используемая в помещениях организации.

Пример - Сервер, микрокомпьютер, используемый в качестве рабочей станции.

Периферийное обрабатывающее оборудование. Аппаратура, подсоединенная к компьютеру посредством связного порта (соединение через последовательные, параллельные каналы и т. п.) для ввода, перемещения или передачи данных.

Пример - Принтер, сменный дисковод. Носитель данных (пассивный)

Это носители для хранения данных или функций.

Электронный носитель. Носитель информации, который может быть подсоединен к компьютеру или компьютерной сети для хранения данных. Несмотря на компактный размер, такие носители могут содержать большой объем данных. Они могут использоваться со стандартной вычислительной аппаратурой.

Пример - Гибкие диски, CD ROM, резервный картридж, сменный жесткий диск, ключ защиты памяти, магнитная лента.

Другие носители. Статичные, неэлектронные носители, содержащие данные.

Примеры - Бумага, слайд, диапозитив, документация, факс.

Программное обеспечение. Программное обеспечение включает программы, содействующие работе устройства по обработке данных.

Операционная система. Такое наименование подразумевает включение всех программ компьютера, создающего операционную основу, на которой исполняются все другие программы (сервисы или приложения). Оно означает включение ядра и основных функций или сервисов. В зависимости от архитектуры операционная система может быть монолитной или состоящей из микроядра и совокупности системных сервисов. Главными элементами операционной системы являются все сервисы менеджмента оборудования (центральное процессорное устройство, запоминающее устройство, диски и сетевые интерфейсы), сервисы менеджмента задач или процессов, а также сервисы менеджмента пользователей и прав пользователей.

Программное обеспечение обслуживания, сопровождения или администрирования. Программное обеспечение дополняет сервисы операционной системы, но не обслуживает непосредственно пользователей или приложения (даже если это обычно является важным или обязательным для общей работы информационной системы).

Пакетное программное обеспечение или стандартные программы. Стандартные программы или пакетное программное обеспечение являются завершенными продуктами, предназначенными для получения прибыли (а не одноразовыми или специфическими разработками), продаваемыми вместе с носителем, версией и сопровождением. Они обеспечивают сервисы для пользователей и приложений, но не являются персонифицированными или специфичными в отличие от бизнесприложений.

Пример - Программное обеспечение управления базой данных, программное обеспечение электронного обмена сообщениями, программное обеспечение коллективного пользования, программное обеспечение каталогов, программное обеспечение Web-сервера и т.д.

Бизнес-приложение. Стандартное бизнес-приложение. Коммерческое программное обеспечение, предназначенное для предоставления

пользователям прямого доступа к сервисам и функциям, требуемым ими от своей информационной системы в своем профессиональном контексте.

Существует огромное разнообразие видов такого программного обеспечения.

Пример - Программное обеспечение учетных записей, программное обеспечение управления станками, программное обеспечение медицинского наблюдения за пациентами, программное обеспечение менеджмента компетентности персонала, административное программное обеспечение и т.д. Специфическоебизнес-приложение. Программное обеспечение, в котором различные аспекты (главным образом, поддержка, сопровождение, модернизация и т.д.) были разработаны специально для предоставления пользователям прямого доступа к сервисам и функциям, требуемым ими от своей информационной системы. Существует огромное разнообразие видов такого программного обеспечения.

Пример - Менеджмент счетов клиентов операторов дальней связи, приложение мониторинга запуска ракет в реальном времени.

Сеть. Тип "сеть" состоит из всех телекоммуникационных устройств, используемых для соединения нескольких физически удаленных компьютеров или элементов информационной системы.

Среда и поддержка. Среда или оборудование связи и дальней связи характеризуются, главным образом, физическими и техническими характеристиками оборудования ("точка-точка", ретрансляция) и протоколами связи (канальный или сетевой - уровни 2 и 3 семиуровневой модели взаимодействия открытых систем).

Пример - Коммутируемая телефонная сеть общего пользования (PSTN - Public Switching Telephone Network), Ethernet, Gigabit Ethernet, асимметричная цифровая абонентская линия (ADSL - Asymmetric Digital Subscriber Line), стандарты на беспроводную связь (например, WiFi 802.11), спецификация Bluetooth, стандарт FireWire.

Пассивные или активные ретрансляторы. Данный подтип включает все устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы характеризуются поддерживающими сетевыми протоколами связи. В дополнение к базовому ретранслятору они зачастую обеспечивают функции и сервисы маршрутизации и/или фильтрации с использованием связных коммутаторов и маршрутизаторов с фильтрами.

Управление ими зачастую может осуществляться на расстоянии, и обычно они способны генерировать журналы регистрации

Пример - Мост, маршрутизатор, концентратор, коммутатор, автоматический коммутатор каналов.

Связной интерфейс. Связные интерфейсы процессоров подсоединены к процессорам, но характеризуются средой и поддерживающими протоколами, любыми установленными функциями фильтрации, регистрации или

генерации предупреждений и их функциональными возможностями, а также возможностью и необходимостью удаленного управления.

Пример - Пакетная радиосвязь общего назначения (GPRS - General Packet Radio Service), Ethernetадаптер.

Персонал. Тип "персонал" состоит из всех групп сотрудников, участвующих в работе информационной системы. Лицо, принимающее решения. Лицами, принимающими решения, являются владельцы основных активов (информации и функций) и руководители организации или определенного проекта.

Пример - Высшее руководство, руководитель проекта.

Пользователи. Пользователями является персонал, обрабатывающий чувствительные элементы в контексте своей деятельности и несущий в этой связи определенную ответственность. Они могут обладать особыми правами доступа к информационной системе, необходимыми им для решения своих повседневных задач.

Пример - Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска.

Персонал по эксплуатации и сопровождению. Это персонал, занимающийся эксплуатацией и сопровождением информационной системы. Он обладает особыми правами доступа к информационной системе, необходимыми ему для решения своих повседневных задач.

Пример - Системный администратор, администратор данных, оператор резервирования, справочного стола, развертывания приложений, сотрудники службы безопасности.

Разработчики. Разработчики занимаются разработкой приложений организации. Они обладают высокоуровневыми правами доступа к части информационной системы, но не выполняют какихлибо действий в отношении данных, связанных с выпуском продукции.

Пример - Разработчики бизнес-приложений.

Место функционирования организации. Тип "место функционирования организации" включает в себя все площадки, имеющие отношение к области применения или части области применения, и физические средства, необходимые для ее функционирования.

Внешняя среда. Внешней средой являются все места, в которых не могут применяться средства обеспечения безопасности организации.

Пример - Жилища персонала, помещения другой организации, среда за пределами места функционирования организации (городская зона, опасная зона).

Владения организации. Это пространство ограничивается периметром организации, непосредственно контактирующим с внешней средой. Речь может идти о физической защитной границе, обеспечиваемой созданием

физических барьеров, или о средствах наблюдения, установленных вокруг зданий.

Пример - Штат организации, здания.

Зона. Зона создается физической защитной границей, образующей отдельные участки на территории организации. Она обеспечивается с помощью создания физических барьеров вокруг инфраструктур обработки информации организации.

Пример - Офисы, зарезервированная зона доступа, безопасная зона.

Основные сервисы. Все сервисы, необходимые для функционирования оборудования организации.

Связь. Телекоммуникационные сервисы и оборудование, обслуживаемые оператором.

Пример - Телефонная линия, АТС организации с исходящей и входящей связью, внутренние телефонные сети.

Коммуникации. Сервисы и средства (источники и электропроводка), необходимые для снабжения энергией информационно-технологического оборудования и периферийных устройств:

Пример - Источники электропитания с низким напряжением, инвертор, распределительное устройство электрической цепи.

– водоснабжение;

– удаление отходов;

– сервисы и средства (оборудование, контроль) для охлаждения и очистки воздуха.

Пример - Трубы водяного охлаждения, кондиционеры воздуха.

Организация. Тип "организация" связан с описанием схемы организации, состоящей из всех кадровых структур, выполняющих некую работу, и процедур, управляющих этими структурами.

Административные органы. Структуры, от которых указанная организация получает свои полномочия. Они могут быть юридически оформленными филиалами организации или внешними структурами. Это налагает ограничения на оцениваемую организацию в плане правил, решений и действий.

Пример - Контролирующая организация, правление организации.

Структура организации. Она состоит из различных отделений организации, включая деятельность организации с пересекающимися функциями под управлением ее руководства.

Пример - Кадровый менеджмент, менеджмент ИТ, снабженческий менеджмент, менеджмент бизнес-подразделений, служба безопасности зданий, пожарная служба, менеджмент аудита.

Организация проекта или системы. Организация, созданная для определенного проекта или сервиса.

Пример - Проект разработки нового приложения, проект миграции информационной системы.

Контрагенты/поставщики/изготовители. Организация, обеспечивающая данную организацию сервисом или ресурсами и связанная с ней договором.

Пример - Компания по управлению оборудованием, аутсорсинговая компания, консалтинговые компании.

2 Установление ценности активов

Следующий шаг после определения активов состоит в согласовании используемой шкалы ценностей и критериев для присвоения каждому активу определенного положения на шкале, основанного на установлении ценности. Вследствие разнообразия активов, встречающихся в большинстве организаций, вероятно, что некоторые активы, имеющие известную денежную ценность, будут оценены в единицах местной валюты, тогда как другим, обладающим в большей степени качественной ценностью, может быть присвоена ценность, колеблющаяся, например, в пределах от "очень низкой" до "очень высокой". Решение о том, какую шкалу использовать, количественную или качественную, в действительности является вопросом предпочтения организации, но она должна быть уместна для оцениваемых активов. Оба вида определения ценности могут быть использованы для одного и того же актива.

Типичные термины, используемые для качественного установления ценности активов, включают следующие определения: пренебрежимо малая, очень низкая, низкая, средняя, высокая, очень высокая, критичная. Выбор и диапазон терминов, подходящих для организации, сильно зависят от потребности в безопасности организации, размера организации и других, характерных для организации факторов.

Критерии. Критерии, используемые в качестве основы для присвоения ценности каждому активу, должны быть записаны в однозначных выражениях. Это часто является одним из наиболее сложных аспектов установления ценности активов, поскольку ценность некоторых активов, возможно, должна устанавливаться субъективно и принимать решения, вероятно, будут разные люди. Возможные критерии, используемые для определения ценности актива, включают его исходную стоимость, стоимость его замены или воссоздания, или ценность, которая может быть абстрактной, например ценность репутации организации.

Еще одной основой для установления ценности активов являются расходы, понесенные из-за потери конфиденциальности, целостности и доступности в результате инцидента. Неотказуемость, учетность, подлинность и надежность также должны рассматриваться соответствующим образом. Такое установление ценности обеспечит изменения важных элементов ценности актива в дополнение к восстановительной стоимости, основанных на

приблизительных оценках неблагоприятных последствий для бизнеса, вытекающих из инцидентов безопасности с предполагаемой совокупностью обстоятельств. Следует подчеркнуть, что при этом подходе принимаются во внимание последствия, которые необходимо включать в оценку риска.

Многим активам в ходе установления ценности могут присваиваться несколько значений ценности. Например, бизнес-план может оцениваться на основе труда, затраченного на его разработку, он может оцениваться на основе труда, необходимого для ввода данных, или он может оцениваться на основе его значимости для конкурентов. Все эти присвоенные значения ценности скорее всего будут существенно различаться. Присвоенное значение может быть максимальным из всех возможных значений или суммой некоторых или всех возможных значений. В окончательном анализе должно быть тщательно определено, какое значение или значения ценности присваиваются активу, потому что окончательная присвоенная ценность включается в определение ресурсов, которые должны быть затрачены на защиту актива.

Сведение к общей основе. В конечном счете все установления ценности активов должны быть сведены к общей основе. Это можно сделать с помощью критериев, приведенных ниже. Критерии, которые могут использоваться для оценки возможных последствий, вытекающих из потери конфиденциальности, целостности, доступности, неотказуемости, учетности, подлинности или надежности активов, включают:

- нарушение законодательства и/или норм;
- ухудшение функционирования бизнеса;
- потеря "неосязаемого капитала"/негативное влияние на репутацию;
- нарушения, связанные с личной информацией;
- создание угрозы личной безопасности;
- неблагоприятное влияние на обеспечение правопорядка;
- нарушение конфиденциальности;
- нарушение общественного порядка;
- финансовые потери;
- нарушение бизнес-деятельности;
- создание угрозы для безопасности окружающей среды.

Другим подходом к оценке последствий могут быть:

- прерывание сервиса - невозможность обеспечения сервиса;
- утрата доверия клиента - утрата доверия международной информационной системе, потеря репутации;
- нарушение внутреннего функционирования - нарушения внутри самой организации, дополнительные внутренние расходы;
- нарушение функционирования третьей стороны - нарушения в функционировании третьих сторон, ведущих дела с организацией, различные виды убытков;

– нарушение законов/норм - неспособность выполнения правовых обязательств;

– нарушение договора - неспособность выполнения договорных обязательств;

– опасность для персонала/безопасность пользователей - опасность для персонала и/или пользователей организации;

– вторжение в частную жизнь пользователей;

– финансовые потери;

– финансовые потери, связанные с чрезвычайными обстоятельствами или ремонтом – касающиеся персонала, касающиеся оборудования, касающиеся исследований, отчетов экспертов;

– потеря товаров/фондов/активов;

– потеря клиентов, потеря поставщиков;

– судебные дела и штрафы;

– потеря конкурентного преимущества;

– потеря технологического/технического лидерства;

– потеря эффективности/надежности;

– потеря технической репутации;

– снижение способности к заключению соглашений;

– промышленный кризис (забастовки);

– правительственный кризис;

– увольнения;

– материальный ущерб.

Эти критерии являются примерами проблем, которые должны рассматриваться при установлении ценности активов. Для проведения оценок организации нужно выбрать критерии, уместные для ее вида бизнеса и требований безопасности. Это может означать, что некоторые из перечисленных выше критериев неприменимы и может потребоваться дополнение к этому списку.

Шкала. После установления критериев для рассмотрения организации следует согласовать шкалу, которая будет использоваться в масштабах организации. Первым шагом является принятие решения о числе используемых уровней. Не существует правил, определяющих наиболее уместное число уровней. Большее число уровней обеспечивает больший уровень детализации, но иногда слишком мелкая дифференциация затрудняет присвоение согласованных оценок в масштабе организации. Обычно может использоваться любое число уровней от 3 (например, низкий, средний и высокий) до 10 в соответствии с подходом, используемым организацией для всего процесса оценки риска.

Организация может установить собственные пределы ценности

активов, такие, как "низкий", "средний" или "высокий". Эти пределы должны оцениваться в соответствии с выбранными критериями, (так, для возможных финансовых потерь пределы должны быть указаны в денежном выражении, но при рассмотрении, например угрозы личной безопасности, определить их денежную ценность может быть затруднительно и неприемлемо для всех организаций). Наконец, решение о том, что считать незначительными или серьезными последствиями, полностью зависит от организации. Последствия, катастрофические для небольшой организации, могут быть незначительными или даже пренебрежимо малыми для очень крупной организации.

Зависимости. Чем более значимые и многочисленные бизнес-процессы поддерживаются активом, тем больше ценность этого актива. Должна быть также определена зависимость одних активов от других, поскольку это может влиять на ценность активов. Например, конфиденциальность данных должна сохраняться в течение всего их жизненного цикла, на всех стадиях, включая хранение и обработку, т.е. необходимость обеспечения безопасности хранения данных и программ обработки данных должна быть напрямую связана с ценностью, отображающей конфиденциальность хранящихся и обрабатываемых данных. Также, если бизнес-процесс зависит от целостности определенных данных, создаваемых программой, входные данные этой программы должны иметь соответствующую степень надежности. Кроме того, целостность информации будет зависеть от аппаратных и программных средств, используемых для ее хранения и обработки. Аппаратные средства, в свою очередь, будут зависеть от энергоснабжения и, возможно, от кондиционирования воздуха. Таким образом, информация о зависимостях поможет в определении угроз и особенно в выявлении уязвимостей. Кроме того, это поможет обеспечить правильное присвоение значения ценности активам (благодаря зависимым взаимосвязям), показывая, таким образом, соответствующий уровень защиты.

Ценность активов, от которых зависят другие активы, может изменяться следующим образом:

– если ценность зависимых активов (например данных) ниже или равна ценности рассматриваемого актива (например, программного

обеспечения), его ценность остается такой же;

– если ценность зависимых активов (например данных) выше ценности рассматриваемого актива (например, программного обеспечения), его ценность должна быть увеличена в соответствии со степенью зависимости или ценностью других активов.

У организации могут быть некоторые активы, являющиеся доступными более одного раза, такие, как копии компьютерных программ или компьютеры одного и того же вида, использующиеся в большинстве офисов. Этот факт необходимо учитывать при установлении ценности активов. С одной стороны, эти активы легко упустить из виду, поэтому следует заботиться о том, чтобы

определить каждый из них; с другой стороны, они могут быть использованы для уменьшения проблем доступности.

Результат. Окончательным результатом этого шага будет перечень активов и их ценности по отношению к раскрытию (сохранение конфиденциальности), модификации (сохранение целостности, подлинности, неотказуемости и учетности), недоступности и разрушению (сохранение доступности и надежности) и восстановительной стоимости.

3 Оценка влияния

Инцидент ИБ может оказывать влияние более чем на один актив или только на часть актива. Влияние связано со степенью успешности инцидента. Как следствие, существует важное различие между ценностью актива и влиянием, являющимся результатом инцидента. Влияние рассматривается как имеющее либо незамедлительный (операционный) эффект, либо будущий (бизнес-) эффект, который включает финансовые и рыночные последствия.

Непосредственное (операционное) влияние бывает прямым или косвенным.

Прямое:

– финансовая восстановительная стоимость потерянного актива (части актива);

– стоимость приобретения, конфигурирования и установки нового актива или резервной копии;

– стоимость приостановленных из-за инцидента операций, пока услуга, предоставляемая активом (активами), не будет восстановлена;

– влияние приводит к нарушению ИБ. Косвенное:

– издержки упущенных возможностей (финансовые ресурсы, необходимые для замены или восстановления актива, могли быть использованы где-либо еще);

– стоимость прерванных операций;

– возможное злоупотребление информацией, полученной в результате нарушения безопасности;

– нарушение установленных законом или нормативных обязательств;

– нарушение этических норм поведения.

Первая оценка (без мер и средств контроля и управления любого рода) будет оценивать влияние как очень близкое к ценности связанного с этим актива или комбинации активов. При каждой последующей итерации для этого (этих) актива (активов) влияние будет отличаться (обычно будет гораздо ниже) вследствие наличия и эффективности реализованных мер и средств контроля и управления.

Ход работы

На основании результатов предыдущей практической работы выполнить:

1. Определение активов.
2. Установление ценности активов.
3. Оценка влияния.

Результат выполнения оформить в виде отчёта под названием *ИвановИИ.pdf*.

Пример формы представления результатов выполнения практической работы

Актив	Тип актива (основные/ вспомога-тельные)	Ценность актива				Восстанови тельная стоимость	Влияние	
		Раскрытие	Модификация	Недоступность	Разрушение		Прямое	Косвенное

Практическая работа № 3
ОПРЕДЕЛЕНИЕ СЦЕНАРИЕВ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы – получить навык определения сценариев инцидентов информационной безопасности.

Ход работы

Произвести построение сценариев инцидентов информационной безопасности для активов организации. Сценарий инцидента представить в виде схемы (рисунок 1).

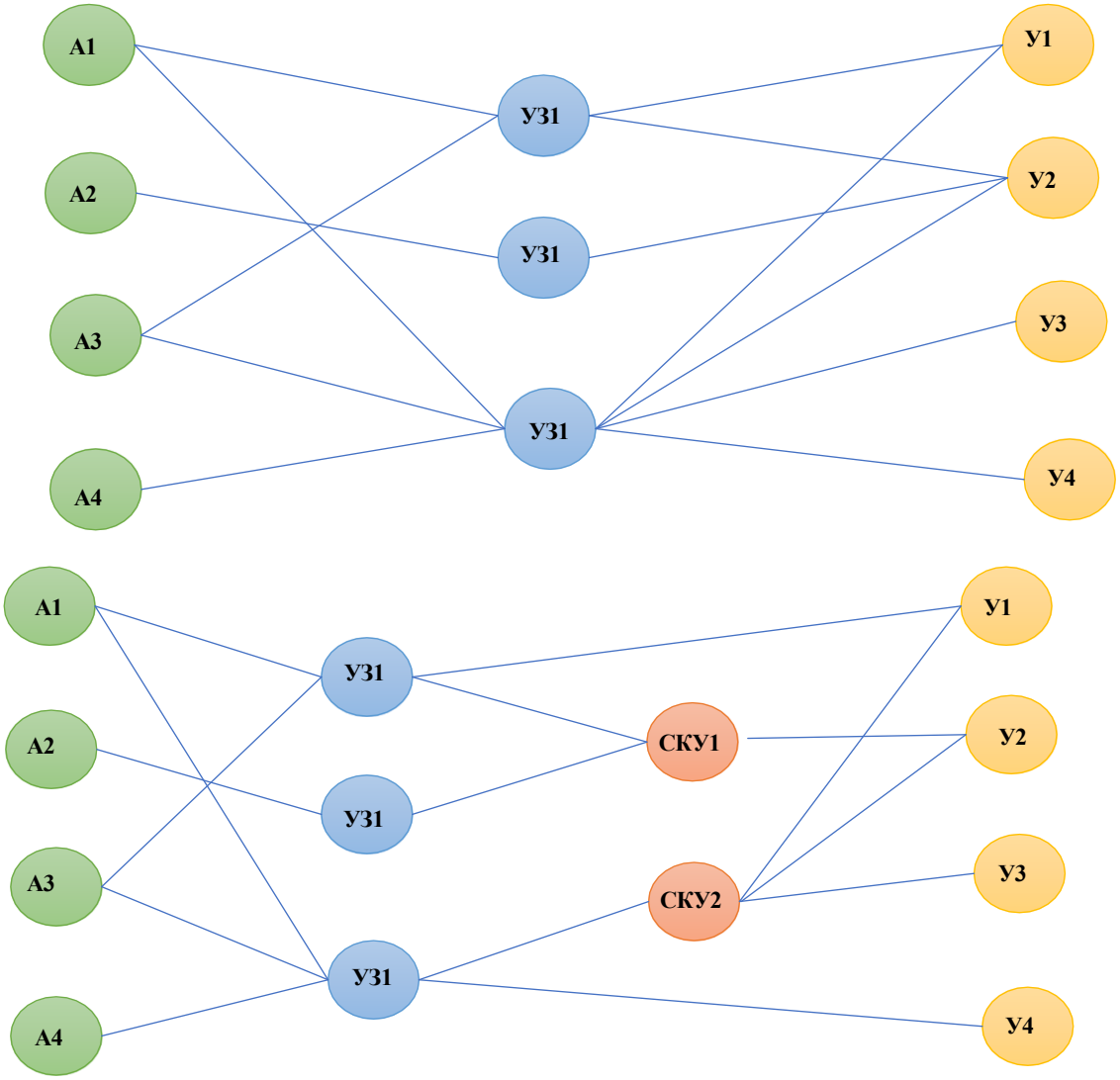

Рисунок 1 - Сценарий инцидентов информационной безопасности для активов организации (А1,2,… – активы; УЗ1,2,… – уязвимости; СКУ1,2,… – средства контроля и управления; У1,2,… – угрозы)

Результат выполнения оформить в виде отчёта под названием *ИвановИИ.pdf*.

Практическая работа № 4
ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы – получить навык оценки рисков информационной безопасности.

Задание. Произвести оценку рисков информационной безопасности, исходные данные к которым получить при помощи метода экспертных оценок. В заключении к работе указать сценарии инцидентов информационной безопасности, для которых риск определен как средний или высокий.

Ход работы

Последствия могут оцениваться несколькими методами, включая использование количественных, например денежных, и качественных мер (которые могут быть основаны на использовании таких прилагательных, как умеренные или серьёзные) или их комбинации. Для оценки вероятности возникновения угрозы должны быть установлены временные рамки, в течение которых актив будет обладать ценностью или нуждаться в защите. На вероятность возникновения конкретной угрозы оказывает влияние следующее:

– привлекательность актива или возможное воздействие - применимо при рассмотрении умышленной угрозы со стороны персонала;

– простота преобразования, использующего уязвимость, актива в вознаграждение - применимо при рассмотрении умышленной угрозы со стороны персонала;

– технические возможности действующего фактора угрозы - применимо при рассмотрении умышленной угрозы со стороны персонала;

– чувствительность уязвимости к использованию - применимо к техническим и нетехническим уязвимостям.

Определение ценности актива выполняется с использованием принципов определения ценности информации, которые охватывают такие вопросы, как:

– личная безопасность;
– юридические и регулятивные обязательства;
– правоприменение;
– коммерческие и экономические интересы;
– финансовые потери/нарушение деятельности;
– общественный порядок;
– политика и операции бизнеса;

– потеря "неосязаемого капитала";
– договор или соглашение с клиентом.

Принципы облегчают идентификацию значений ценности на числовой шкале, как, например, на шкале от 0 до 4, показанной в приведённом ниже примере (см. таблицу ниже), делая, таким образом, возможным присвоение количественных значений, если это возможно и обоснованно, и качественных значений, где количественные значения невозможны, например, в случае создания опасности для человеческой жизни.

Следующим важным мероприятием является заполнение ряда опросных листов для каждого вида угрозы, каждой группы активов, с которой связан данный вид угрозы, чтобы сделать возможной оценку уровней угроз (вероятности возникновения) и уровней уязвимостей (простоты использования угрозами, чтобы вызвать неблагоприятные последствия). Каждый ответ на вопрос даёт баллы. Эти баллы складываются, используя базу знаний, и сравниваются с диапазонами. Это идентифицирует уровни угроз, скажем, на шкале от высокой до низкой и, аналогично, уровни уязвимостей, как показано в приведённом ниже примере таблицы, проводя различия между видами последствий, как будет уместно. Информация для заполнения опросных листов должна собираться из опросов соответствующего технического персонала, представителей отдела кадров, из данных инспекций фактического месторасположения и проверки документации.

Ценность активов, уровни угроз и уязвимостей, относящиеся к каждому виду последствий, приводятся к табличной форме (матрице), такой как представлена ниже, чтобы для каждой комбинации идентифицировать соответствующую меру риска на основе шкалы от 0 до 8.

Таблица 1 - Матрица ценности активов, уровни угроз и уязвимостей, относящиеся к каждому виду последствий.

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для каждого актива рассматриваются уместные уязвимости и соответствующие им угрозы. Если существует уязвимость без соответствующей угрозы или угроза без соответствующей уязвимости, то в настоящее время риск отсутствует (но следует проявлять осторожность в

случае изменения этой ситуации). Теперь соответствующая строка в таблице устанавливается по значению ценности актива, а соответствующая колонка устанавливается по вероятности возникновения угрозы и простоте использования. Например, если актив имеет ценность 3, угроза является "высокой", а уязвимость "низкой", то мера риска будет равна 5.

Данная шкала рисков может также отображаться для простого общего рейтинга рисков, например, следующим образом:

- низкий риск: 0-2;
- средний риск: 3-5;
- высокий риск: 6-8.

Для реализации данной методики актуально использовать следующую таблицу:

Таблица 2 - Соответствие активов и угроз

Актив	Ценность актива	Инцидент ИБ	Вероятность возникновения угрозы	Простота реализации	Последствия реализации угрозы

Для заполнения данной таблицы следует использовать шкалы, приведенные выше.

Результат выполнения оформить в виде отчёта под названием *ИвановИИ.pdf*.

Практическая работа № 5
ОБРАБОТКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы – получить навык обработка рисков информационной безопасности.

Задание

1. Для каждого риска, получившего оценку "Средний риск" и "Высокий риск", определить один из способов управления рисками:
   - предотвращение рисков;
   - сохранение риска;
   - перенос риска;
   - снижение риска.
2. Для каждого риска обосновать выбор способа управления рисками.
3. Осуществить выбор средств управления рисками, соответствующих выбранным способам, и привести обоснование их выбора.

Результат выполнения оформить в виде отчёта под названием *ИвановИИ.pdf*.

СПИСОК ЛИТЕРАТУРЫ

1. Аверченков В.И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с.

2. Веселов Г.Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.

3. Золотарев В.В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.

4. Жукова М.Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с.

У ч е б н о е и з д а н и е

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по практическим работам

Составитель: **Контылева** Елена Александровна

В авторской редакции

Изд. № 119/2025. Объем 2 п. л. Усл. печ. л. 1,86. Уч.-изд. л. 1,96.
Издательский центр ФГАОУ ВО «Севастопольский государственный университет»